DataBridge^{7} LALS

Digital Intelligence

BAE SYSTEMS

Understanding Lawful Access Location Services

Lawful Access Location Services (LALS), as defined in ETSI TS 33.127, establishes a standardised framework for providing subscriber location information to law enforcement agencies (LEAs). It leverages existing communication service provider (CSP) network location service infrastructure (LCS) — including LCS Servers and Gateway Mobile Location Centres (GMLC) while operating under a lawful override of normal privacy protection.

LALS is critically important because it ensures that law enforcement can obtain timely, accurate and lawfully compliant location information when responding to emergencies, investigating serious crimes, or locating missing persons. At the same time, it maintains clear audit trails and strict policy enforcement, preserving the integrity of subscriber privacy for all non-authorised requests.

In short, LALS provides a trusted, regulated bridge between law enforcement needs and mobile network capabilities - enabling lawful, precise and auditable access to location data without compromising network security or privacy standards.

The challenges of direct LCS infrastructure integration

While LALS provides a standardised, lawfully compliant mechanism for LEAs to access subscriber location information, the practical realities of using this capability are complex, fragmented and resource-intensive. The underlying network infrastructure - including position determining network elements - is capable of providing highly accurate, near-real-time location data. Yet, the workflow for requesting and receiving this information remains complex.

Challenges

- **Complexity of Telecom interfaces:** LALS relies on standard network Location Services (LCS) protocols to interact with the core network positioning functions. For LEAs, this means that requests often require specialised technical knowledge of network signalling, interfaces and positioning workflows. Most law enforcement personnel are not telecom experts, and operator support is typically required to translate requests into valid network element procedures. This creates dependency on network staff, slowing response times and increasing operational risk.

- **Fragmentation across networks and vendors:** Mobile networks are heterogeneous: different operators, vendors and technology generations (2G, 3G, 4G, 5G) implement positioning and LCS functions differently. Consequently, lawful location request workflows vary, and each network may deliver results in different formats or through different processes. This fragmentation complicates investigations and increases the risk of errors, delays, or misinterpretation.

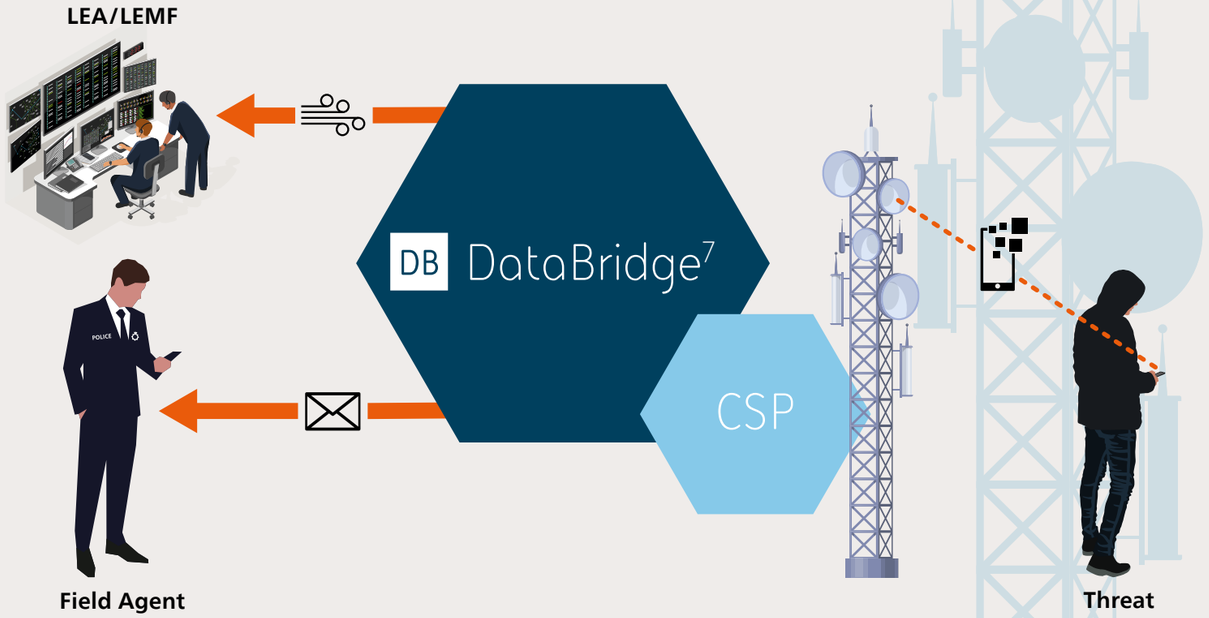
- **Inconsistent location data delivery:** Even when the network returns location information, components such as data formats, accuracy indicators and positioning methods are not standardised across operators. Law enforcement agencies often need to manually interpret or normalise this data to integrate it into investigative systems or operational tools. In urgent situations, such as missing persons or active crime scenes, these delays and inconsistencies can have critical consequences.

- **Operational burden on network CSPs:** From the CSP perspective, fulfilling LALS requests involves manual coordination, validation of lawful authority, privacy checks and audit logging. Each request can consume significant time and resources, particularly when handling high volumes or multiple concurrent requests. This operational burden limits scalability and can delay access to critical information.

- **Time-sensitive nature of investigations:** Lawful location requests are often needed immediately, yet current processes are rarely optimised for speed. The combination of manual workflows, technical complexity and multi-network variation means that LEAs may not receive location information as quickly as needed - potentially impacting investigation outcomes and public safety.

Transforming Lawful Access to subscriber location

Where granular user equipment (UE) location information is required, DataBridge[7] provides LALS capability that conceals the complexity of CSP LCS-Server/GMLC interoperability by providing a complete and fully ETSI compliant end-to-end workflow for LEAs to obtain lawful access to subscriber location. Whether a critical real-time mission or an extended surveillance operation, LEAs can develop strategies using both target positioning and triggered location capability with use of the DataBridge[7] LRS (Location Request Service) and LTF (Location Trigger Function). Combined with the standardised LI_H1 eWarrantry interface, DataBridge[7] WMS or other existing non-standardised surveillance provisioning workflows, DataBridge[7] LALS provides a variety of secure delivery mechanisms for all acquired and mediated LALS location events including IRI over HI2 or email/SMS to authorised field personnel.

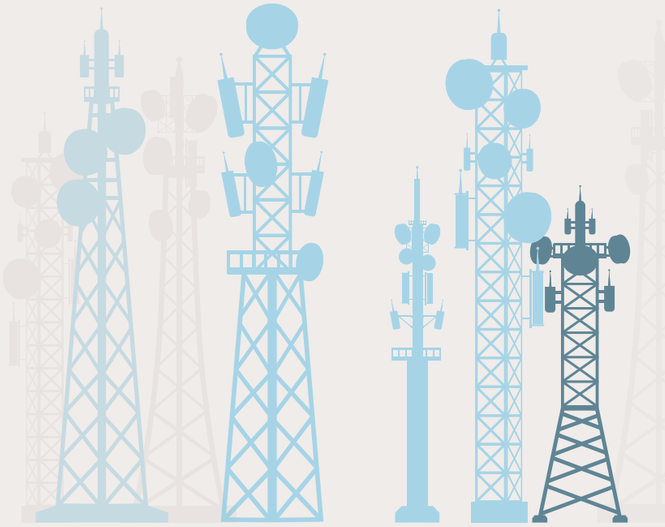


Target Positioning - Immediate/periodic location requests

DataBridge[7] LRS REST endpoint enables LEAs to learn a target's positioning using either Location Immediate Request (LIRs) or Periodic Location Requests (PLRs). Where an LIR facilitates a one time only request, a PLR enables LEAs to issue a single request object that instructs the LI-LCS Client to periodically execute location requests against the LCS Server/GMLC for a LEA defined period and duration. A LALS Report detailing the surveillance positioning is delivered to the requesting LEA/LEMF for every request issued to the LCS Server/GMLC.

Triggered Surveillances

In addition to immediate and periodic request capability, DataBridge[7] LTF enables LEAs to provision LALS Trigger surveillances where upon the receipt of selected triggerable IRI events attributed to the surveillance (such as e-UTRAN attach or call-establishment IRI events), a request is issued by the LI-LCS Client to the LCS Server/GMLC and a LALS Report is delivered in association with the triggered IRI event. By using LALS Triggered Surveillances, DataBridge[7] supports the acquisition of accurate geo-location information of mobile devices that are only momentarily attached to the CSP network.



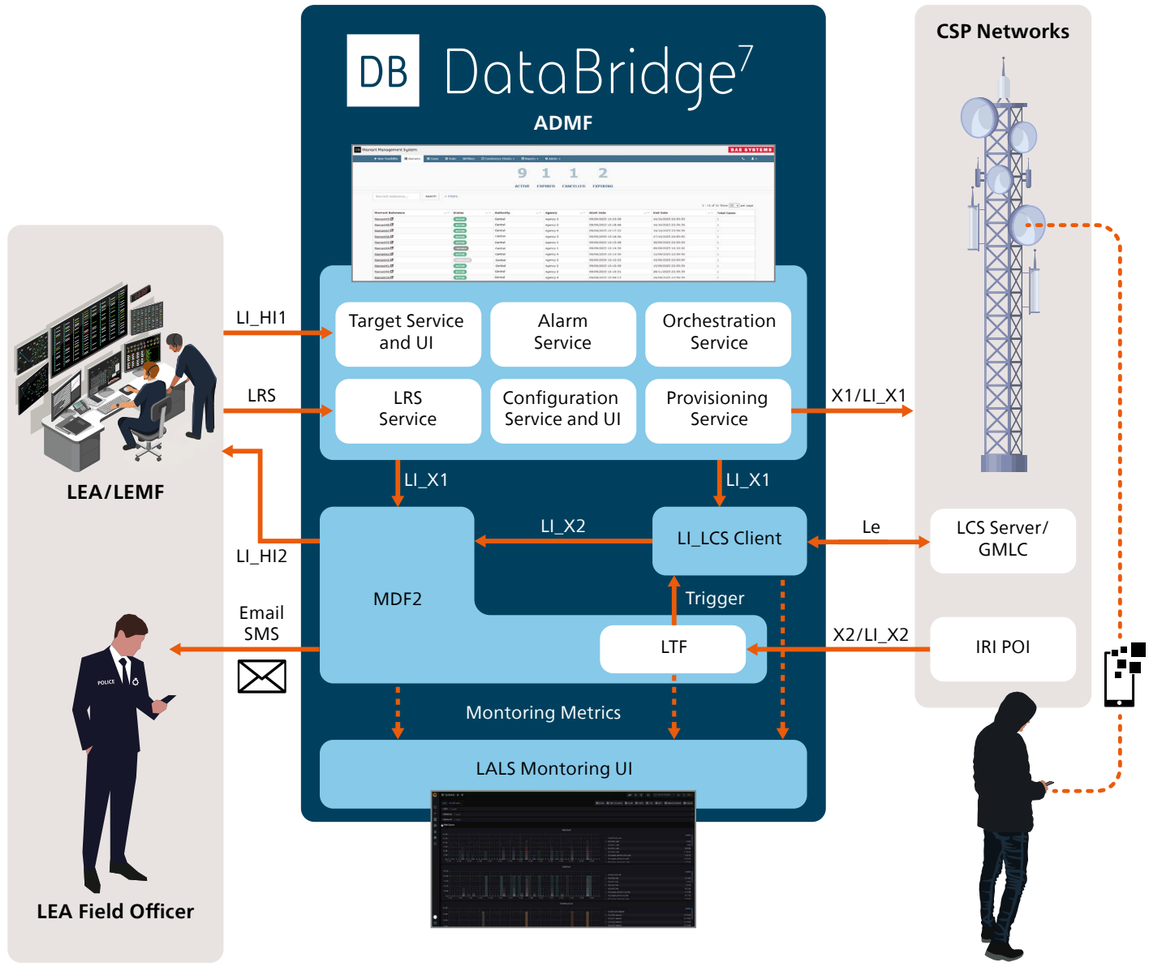


Figure 1: *DataBridge[7] LALS Architecture*

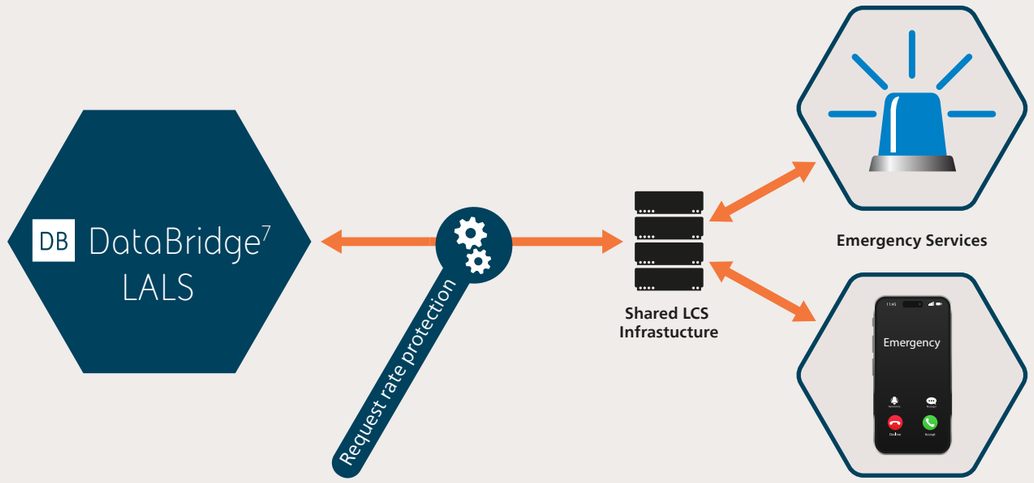


Figure 2: *DataBridge[7] Request Rate Protection Capability*

DataBridge[7] LALS Administration

DataBridge[7] LALS capability can exist standalone, inheriting all DataBridge[7] product functionality or as an extension to an existing DataBridge[7] LI platform. Surveillance administration of DataBridge[7] LALS may be performed using either of the following:

- **DataBridge[7] WMS (Warrant Management System) -** provides a secure, flexible and intuitive web UI platform for warrant administration that is specifically designed to meet the requirements of warrant data entry, authorisation, automated network provisioning, auditing and reporting.

- **ETSI TS 103.120 LI_HI1 eWarrantry service -** enables LEAs to manage warrants and surveillances via machine-to-machine interface using TS 103.120 LITaskObjects and other standardised objects and workflows.

In addition to the above surveillance administration workflows, DataBridge[7] LALS includes DataBridge[7] Architect, an intuitive web UI platform purposed with environment setup and configuration management of all system and software modules. In the context of LALS, relevant configuration includes IRI trigger event selection, GMLC throttling parameters, LI-LCS caching settings and more.

Request and Response Caching

DataBridge[7] conceals the complexity of LCS asymmetrical request and response behaviours and delayed responses through the use of a location request and response cache. DataBridge[7] LALS intelligently manages inbound and outbound requests to prevent unnecessary duplicate requests and the creation of unexpected duplicate LALS HI responses sent to LEMFs or LEA Field Officers over email/SMS.

Request Rate Control

Existing CSP LCS infrastructure may enforce strict limits on the number of location requests that can be processed per second. Exceeding these limits can not only lead to failed requests, but also risk disrupting other critical services such as emergency response systems, which rely on the same LCS infrastructure for urgent location data. For law enforcement applications, uncontrolled or 'bursty' traffic could unintentionally impact these high-priority services, creating a significant operational and safety risk.

DataBridge[7] LALS is built with this appreciation in mind and employs Request Rate Control capability. Where multiple thousands of live surveillances may be provisioned and active, intelligent request rate control and distribution by DataBridge[7] LALS ensures that a high volume of requests due to both Periodic Location Requests (PLRs) and non-deterministic IRI based Triggered Surveillances are appropriately queued, prioritised and distributed over time. This protects both the network and other critical service clients, allowing law enforcement to access accurate location information safely while maintaining the reliability of emergency services and other critical applications.

LALS Monitoring

DataBridge[7] provides real-time and retained granular statistics to keep system operators informed of all LALS activity over a desired period range.

DataBridge[7] DBStats provides the following LALS statistics and visualisations:

- Real-time and historical request count including Trigger Events count
- Real-time and historical record cache count
- Graphical view into any ongoing request queuing and cleardown times
- Total number of LCS-Server/ GMLC response records processed
- Real-time LCS-server/GMLC response latency timing
- Graphical view of historical LALS Trigger Events against time
- LALS Trigger Event count by specific IRI events

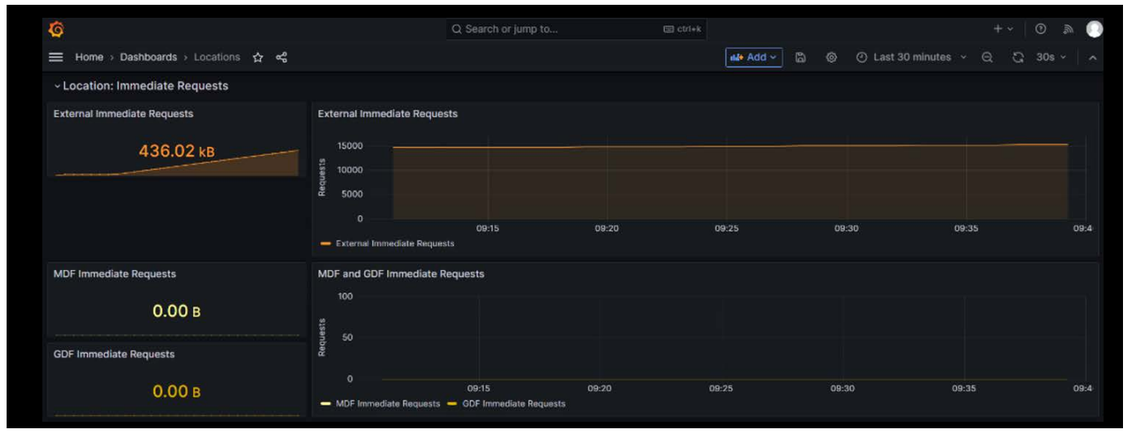


Figure 3: *LIR Request Count visualisation*

Technical Specifications

Supported Interfaces

DataBridge[7] LALS capability is fully compliant with the following standardised interfaces:

- **Le -** support for legacy and current versions of OMA-TS-MLP Le interface protocol
- **LI_HI1 -** compliant with ETSI TS 103.120 LI warrant interface specification
- **LI_HI2 -** compliant with ETSI TS 102 232 specifications. LALS payload support for:
  - ETSI TS 133.128 LALS Report Record including positioninfo support for all GeographicArea defined shapes and measurements.
  - ETSI TS 133.108 LALS Target Positioning Report Record with GAD wGS84 shape encodings.
- **Email -** support for all common email protocols
- **SMS -** support for SMS gateway services or air gapped SMS
- **X1/LI_X1 -** compliant with ETSI TS 103 221-1. DataBridge[7] core solution X1 support for a variety vendor technologies in all communication domains including fixed line broadband, PSTN voice, GPRS, GSM, UMTS, LTE, NR and satellite voice.
- **X2/LI_X2 -** compliant with ETSI TS 103 221-2. DataBridge[7] base LI solution X2 support for a variety vendor technologies in all communication domains including fixed line broadband, PSTN voice, GPRS, GSM, UMTS, LTE, NR and satellite voice. All X2/LI_X2 IRI messages supported as LALS triggerable events.

We are Digital Intelligence

Digital Intelligence is home to over 4,700 digital, cyber and intelligence experts across 16 countries. We operate at the cutting edge of digital innovation and at the heart of organisations that keep vital infrastructure running, national security protected and armed forces prepared.

Our teams provide advanced digital capability, products and solutions that weave together digital threads of data so that customers get the vital insight they need – from the fine detail to the bigger picture, providing the power of perspective to confidently make the critical decisions that keep our societies safe and able to thrive.

Digital Intelligence is part of BAE Systems and has a rich heritage in helping to defend nations and businesses around the world from advanced threats. Whether on land, in the air, at sea, in space or cyberspace, we're your digital mission partner, with you every step of the journey.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS